REMARKS

Initially, in the Office Action dated June 3, 2004, the Examiner rejects claims 1-5 and 7-12 under 35 U.S.C. §112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which Applicants regard as the invention. Claims 2, 3, 8 and 9 have been rejected under 35 U.S.C. §101 because the claimed invention is directed to non-statutory subject matter. Claim 6 has been rejected under 35 U.S.C. §102(a) as being anticipated by EP 0 874 307 A1 (Vanstone et al.). Claim 6 has been rejected under 35 U.S.C. §102(b) as being anticipated by "An Implementation of Elliptic Curve Cryptosystems Over F2155", pp. 804-813 (Agnew et al.). Claims 2, 3, 8 and 9 have been rejected under 35 U.S.C. §103(a) as being unpatentable over Vanstone et al. in view of "Sequences of Numbers Generated by Addition in Formal Groups and New Primality and Factorization Tests" (Chudnovsky et al.).

By the present response, Applicant has amended claims 1, 3, 8 and 9 to further clarify the invention. Claims 2, 3, 6, 8 and 9 remain pending in the present application.

35 U.S.C. §112 Rejections

Claims 1-5 and 7-12 have been rejected under 35 U.S.C. §112, second paragraph. Applicant has amended these claims to further clarify the invention and in accordance with the Examiner's suggestion and, therefore, these rejections have now been overcome. Applicant respectfully request that these rejections be withdrawn.

35 U.S.C. §101 Rejections

Claims 2, 3, 8 and 9 have been rejected under 35 U.S.C. §101. Applicant has amended these claims to further clarify the invention and to recite that the method includes steps/operations performed by a cryptographic apparatus. This is clearly statutory subject matter. Applicant respectfully request that these rejections be withdrawn.

35 U.S.C. 102 Rejections

Claim 6 has been rejected under 35 U.S.C. §102(a) as being anticipated by Vanstone et al. Applicant has discussed the deficiencies of Vanstone et al. in Applicant's previously-filed response and reassert all arguments submitted in that response. Applicant respectfully traverses this rejection and provides the following additional remarks.

Regarding claim 6, Applicant submits that Vanstone et al. does not disclose or suggest the limitations in the combination of this claim of, inter alia, an apparatus implementing an elliptic curve cryptographic operation that includes random number generating means for generating a random number k and projective coordinate transformation means receiving as inputs thereto coordinate x0 of the finite field of characteristic 2 and the random number k, to thereby transform the coordinate x0 into projective coordinates $[kx0, k] = [x_1, z_1]$. It appears that the Examiner still fails to understand the limitations in the claims of the present invention. The Examiner again fails to issue a proper §102 rejection--that requires the Examiner to specifically point out portions in a cited reference that the Examiner asserts discloses or suggests a limitation in the claims of the present application--but merely references

four pages of the Vanstone et al. reference (pages 5-8). As has been noted previously, these pages of Vanstone et al. merely disclose the multiplication method of Vanstone et al. These portions do not disclose or suggest a random number generating means for generating a random number k or projective coordinate transformation means receiving as inputs thereto coordinate x0 of a finite field of characteristic 2 and a random number k to thereby transform the coordinate x0 into projective coordinates $[kx0, k] = [x_1, z_1]$, as recited in the claims of the present application. Vanstone et al. merely discloses that k (24 in Fig. 2) is described as "kP" (see Vanstone specification, page 7, second paragraph). This represents an arithmetic of a scalar multiplication relative to a point P on an elliptic curve. In contrast, as exemplified in claim 6 of the present invention, k represents an arithmetic value [kx0, k] relative to components of projective coordinates, which is not a scalar. According to the present invention, a random number k is multiplied to respective components of projective coordinates [x0, 1]. The values of the components will change when the components are subjected to division by the random number. However, the point indicated by the coordinates does not change. Thus, by changing the component value of the projective coordinate randomly, the operand value for arithmetic operation is changed randomly, thereby defending a timing attack. Similarly, each of claims 2 and 8 (although not rejected here) defines projective coordinate $[k^2x, k]$ where k represents a random number. The random number k is multiplied to components of projective coordinates.

In accordance with 35 U.S.C. §102 and in compliance with the MPEP, Applicant respectfully request the Examiner to specifically point out where it is

disclosed in Vanstone et al.: random number generating means for generating a random number k; projective coordinate transformation means receiving as inputs thereto coordinate x0 of said finite field of characteristic 2 and said random number k, to thereby transform said coordinate x0 into projective coordinates [kx0, k] = [X_1, $Z_{,1}$]; doubling arithmetic means for arithmetically determining a double point from said projective coordinates [X_1, Z_1]; addition arithmetic means for determining an addition point from said projective coordinate [X_1, Z_1] where Z is a variable in the z-coordinate to thereby output said addition point; and scalar multiplication means receiving information from said projective coordinate transformation means, said doubling arithmetic means and said addition arithmetic means to thereby perform scalar multiplication of the coordinate component x0. The Examiner's failure to specifically point out in Vanstone et al. the teaching or suggestion of each of these limitations in the claims of the present application results in this rejection being an improper §102 rejection.

Accordingly, Applicant submits that Vanstone et al. does not disclose or suggest the limitations in the combination of claim 6 of the present application. Applicant respectfully requests that this rejection be withdrawn and that this claim be allowed.

Claim 6 has been rejected under 35 U.S.C. §102(b) as being anticipated by Agnew et al. Applicant has discussed the deficiencies of Agnew et al. in Applicants previously-filed response and reassert all arguments submitted in that response. Applicant respectfully traverses this rejection and provides the following additional remarks.

Again, the Examiner fails to issue a proper §102 rejection in that the Examiner fails to specifically point out in the cited reference where each specific limitation is disclosed or suggested in the cited reference. The Examiner again merely references ALL of the 10 pages of Agnew et al. (pages 804-813). These pages of Agnew et al. disclose the elliptic curve cryptosystems implementation of Agnew et al. These portions do not disclose or suggest a random number generating means for generating a random number k or projective coordinate transformation means receiving as inputs thereto coordinate x0 of a finite field of characteristic 2 and a random number k to thereby transform the coordinate x0 into projective coordinates $[kx0, k] = [x_1, z_1]$, as recited in the claims of the present application. Agnew et al., page 807 discloses an arithmetic operation of "kP". Similar to Vanstone et al., this simply represents an arithmetic of a scalar multiplication relative to a point P on the elliptic curve, where k is often a random number. The same arguments assert previously against Vanstone et al. apply against Agnew et al. as well.

For a proper §102 rejection and to comply with the MPEP, the Examiner MUST specifically point out where it is disclosed in Agnew et al.: random number generating means for generating a random number k; projective coordinate transformation means receiving as inputs thereto coordinate x0 of said finite field of characteristic 2 and said random number k, to thereby transform said coordinate x0 into projective coordinates $[kx0, k] = [X_1, Z_{,1}]$; doubling arithmetic means for arithmetically determining a double point from said projective coordinates $[X_1, Z_1]$; addition arithmetic means for determining an addition point from said projective coordinate $[X_1, Z_1]$ where Z is a variable in the z-coordinate to thereby output said

addition point; and scalar multiplication means receiving information from said projective coordinate transformation means, said doubling arithmetic means and said addition arithmetic means to thereby perform scalar multiplication of the coordinate component x0. The Examiner's failure to specifically point out in Agnew et al. the teaching or suggestion of each of these limitations in the claims of the present application results in this rejection being an improper §102 rejection.

Accordingly, Applicant submits that Agnew et al. does not disclose or suggest the limitations in the combination of claim 6 of the present application. Applicant respectfully requests that this rejection be withdrawn and that this claim be allowed.

35 U.S.C. §103 Rejections

Claims 2, 3, 8 and 9 have been rejected under 35 U.S.C. §103(a) as being unpatentable over Vanstone et al. in view of Chudnovsky et al. Applicant has discussed the deficiencies of Chudnovsky et al. in Applicant's previously-filed response and resubmit all arguments submitted in that response. Applicant respectfully traverses these rejections and provide the following additional remarks.

Applicant submits that neither Vanstone et al. nor Chudnovsky et al., taken alone or in any proper combination, disclose, suggest or render obvious the limitations in the combination of each of these claims of, inter alia, generating a random number k, transforming the x-coordinates into projective coordinates to thereby derive projective coordinates $[k^x, k]$ through arithmetic operation of individual coordinate components of the projective space and the stored random number k, or transforming the x-coordinates into projective coordinates to thereby derive projective coordinates [kx, k] through arithmetic operation of individual coordinate

components of the projective space and the stored random number k. The Examiner admits that Vanstone et al. does not disclose or suggest a random number being used to device projective coordinates, but asserts that Chudnovsky et al. discloses methods for improving the speed of elliptic curves and therefore the Examiner believes the teachings of these two references would render the claims of the present application obvious, if the scope of the claims were clearly defined. However, as noted previously Chudnovsky et al. relates to presenting methods for primality testing and generation of big prime numbers and new versions of factorization methods. Neither Vanstone et al. nor Chudnovsky et al. disclose or suggest generating a random number k, or transforming the x-coordinates into projective coordinates to thereby derive projective coordinates either [kx, k] or [k^2x, k], through arithmetic operation of individual coordinate components of the projective space and the stored random number k, as recited in the claims of the present application. These features according to the present invention, result in randomizing data of coordinate components from applying a generated random number to the respective components. The combination of Vanstone et al. with Chudnovsky et al. under 35 U.S.C. §103 are not applicable to the claimed invention, because the application of a random number in Chudnovsky et al. completely different than and thus teaches away from the application of a random number in Vanstone et al.

Accordingly, Applicant submits that none of the cited references, taken alone or in any proper combination, disclose, suggest or render obvious the limitations in the combination of each of claims 2, 3, 8 and 9 of the present application. Applicant

respectfully requests that these rejections be withdrawn and that these claims be allowed.

In view of the foregoing amendments and remarks, Applicant respectfully submits that claims 2, 3, 6, 8 and 9 are now in condition for allowance. Accordingly, early allowance of such claims is respectfully requested.

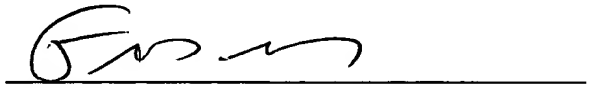
Examiner Interview

After receipt and review of this response, Applicant respectfully requests that the Examiner call Applicant's representative (703 312-6600) to set up an interview. It is hoped at the interview to resolve any issues the Examiner may still have and to allow Applicant's representative to help the Examiner better understand Applicant's claimed invention.

To the extent necessary, Applicants petition for an extension of time under 37 CFR 1.136. Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, or credit any overpayment of fees, to the deposit account of Antonelli, Terry, Stout & Kraus, LLP, Deposit Account No. 01-2135 (referencing attorney docket no. 500.38035X00).

Respectfully submitted,

ANTONELLI, TERRY, STOUT & KRAUS, LLP



Frederick D. Bailey
Registration No. 42,282

FDB/sdb
(703) 312-6600